Schreier G, Hayn D, Ammenwerth E, editors. Tagungsband der eHealth2011. 26.-27.Mai 2011; Wien. OCG; 2011.

QUALIFIZIERTE IDENTIFIKATION VON GESUNDHEITSDIENSTEANBIETERN UNTER VERWENDUNG VON ROLLEN IM GESUNDHEITSWESEN

Danner P[1], Schmid L[1,2], Burgsteiner H[2]

Kurzfassung

Anmeldungen an Gesundheitsanwendungen im extramuralen Bereich verlangen die qualifizierte Identifikation von Gesundheitsdiensteanbietern (GDAs) sowie den Nachweis von deren Rollen. Wir haben ein System entwickelt, das Gesundheitsanwendungen an ein zentrales, gesichertes Register anbindet, und die Überprüfung, sowie den Nachweis von Rollen im Rahmen des Identifikationsprozesses gewährleistet. Die Integration erfolgt in einem sicheren, E-Government konformen Anmeldevorgang, mit der dieser um einen Attribute Provider im Rahmen der Anmeldung erweitert wird.

Abstract

Qualified identification of health professionals (HPs) as well as the proof of their roles has to be ensured during the sign-in process of a health application. We developed a system which connects health applications to a centralized, reliable register to ensure the validation together with the proof of the role within the identification process for a health application. The integration of the solution takes place in a secured, E-Government compliant sign-in procedure and extends this procedure with an Attribute Provider within the sign-in process.

Keywords – eHealth, E-Government, eID, Gesundheitstelematik, IHE

1. Einleitung

Bei der Anmeldung an eine Applikation, die sensible Daten wie Gesundheitsdaten verarbeitet, muss ein Gesundheitsdiensteanbieter (GDA) im Allgemeinen seine Identität und seine Rolle nachweisen. Dieser Nachweis muss in elektronischer Form erbracht werden. GDAs, die nicht an das Gesundheitsinformationsnetz (GIN) angeschlossen sind, benötigen für den Nachweis der eigenen Identität sowie der Rolle eine Anmeldung mittels Bürgerkarte. In dem Begutachtungsentwurf zur Gesundheitstelematikverordnung (GTelV) [3]war der Nachweis von Identität und Rollen eines GDAs mittels einer signierten XML-Struktur namens GDA-Token [1] angedacht. Diese Verordnung kam allerdings nicht über den Status der Begutachtung hinaus, zeigt aber die Intention und Richtung der Legislative. Der Nachteil dieses Konzeptes liegt vor allem in der Abhängigkeit von einer Bürgerkartenumgebung (BKU) 04,8]. GDA-Token müssen in die Infobox einer BKU abgelegt werden. Da

1 exthex GmbH, Göstinger Straße 213, 8051 Graz, AUSTRIA
2 FH Joanneum, Department of eHealth, Eggenberger Allee 11, 8020 Graz, AUSTRIA

es mit den aktuellen Bürgerkartenregelungen derzeit nicht möglich ist, Daten auf einer Smartcard zu speichern, sind GDA-Token danach nur lokal in der BKU verfügbar. Bei der Verwendung verschiedener PCs für die Anmeldung mittels Bürgerkarte müssen die GDA-Token auf allen PCs verfügbar gemacht werden. Laut dem aktuellen Gesundheitstelematikgesetz (GTelG) (BGBl I Nr. 179/2004) können Rollen mittels Vorlage einer elektronischen Bescheinigung (Zertifikat) oder durch Abfrage des eHealth-Verzeichnisdienstes nachgewiesen werden. Die Abfrage des eHealth-Verzeichnisdienstes müsste allerdings auf Seite der Applikation implementiert werden, was als Anforderung für die Entwicklung von Applikationen im Gesundheitswesen gesehen werden kann. Um den erwähnten Nachteilen der lokalen Verfügbarkeit von GDA-Token sowie der notwendigen Implementierung einer Abfrage des Verzeichnisdienstes entgegenzuwirken, wurde ein Identifikations- bzw. Anmeldesystem für GDAs auf Basis der Bürgerkarte und dem Modul für Identifikation MOA-ID (Module für Online Applikationen – ID) [11] entwickelt, welches es erlaubt, die Identität eines GDAs nachzuweisen, seine Rollen online abzufragen und nach erfolgreicher Identitätsprüfung diese Daten an die anfragende Gesundheitsanwendung zu übergeben.

2. Verwandte Arbeiten

Laut dem aktuellen GTelG können Identität und Rollen eines GDAs mittels Vorlage einer elektronischen Bescheinigung (Zertifikat) oder durch Abfrage des eHealth-Verzeichnisdienstes nachgewiesen werden. Der Begriff "Zertifikat" wird hierbei nicht ausschließlich als X.509 Zertifikat verstanden. In dem Begutachtungsentwurf für die GTelV [3] wird vielmehr das Konzept der GDA-Token als Umsetzung der elektronischen Bescheinigung laut GTelG angedacht. GDA-Token werden über automatisierte Prozesse durch die Standesvertretung oder nach einem elektronisch signierten Antrag eines GDAs ausgestellt, wobei mit dem Antrag gleichzeitig die Aufnahme in den eHealth-Verzeichnisdienst beantragt werden kann. Die Prüfung der Identität eines GDAs erfolgt mittels Registern für physische Personen aus dem E-Government (Stammzahl- und Ergänzungsregister) wobei zur Identifikation der Health Professional Identifier (HPI) verwendet wird. Verantwortlich für die authentische Bestätigung der Zuordnung einer Rolle zu einem GDA sind je nach Rolle unterschiedliche Bestandgeber. GDA-Token können vor Ablauf der zeitlichen Gültigkeit widerrufen oder bei Wegfall der Berechtigungen zur Ausübung einer Rolle gesperrt werden. Eine Suspendierung einer Rolle ist ebenfalls möglich. Während das aktuelle GTelG weiterhin einen eHealth-Verzeichnisdienst vorsieht, werden sowohl im GTelG als auch in der GTelV (BGBl II Nr. 451/2008) GDA-Token nicht erwähnt. Somit bleibt die Definition der elektronischen Bescheinigung (Zertifikat) als Möglichkeit zum Nachweis von Identität und Rollen eines GDA offen. Auch die im Dezember 2010 kundgemachten Änderungen des GTelG (BGBl I Nr. 103/2010) und der GTelV (BGBl II Nr. 464/2010) brachten keine Änderungen in Bezug auf Rollen.

Die IHE Initiative (Integrating the Healthcare Enterprise) spezifiziert in ihrem IT Infrastructure Technical Framework [5] ein Profil namens Cross-Enterprise User Assertion (XUA), welches die Möglichkeit bietet, Behauptungen (Assertions) eines authentifizierten Users in Web-Service Transaktionen über Unternehmensgrenzen hinweg zu kommunizieren. Als wichtigstes Ziel von XUA wird das Security Audit Logging und zu einem geringeren Grad auch die Zugriffskontrolle gesehen. XUA definiert als Akteure (actors) einen X-Service User und einen X-Service Provider sowie die Transaktion Provide X-User Assertion. Als zusätzliche, aber nicht spezifizierte Akteure, werden ein User Authentication Provider und ein X-Assertion Provider definiert (*Abbildung 1*Abbildung).

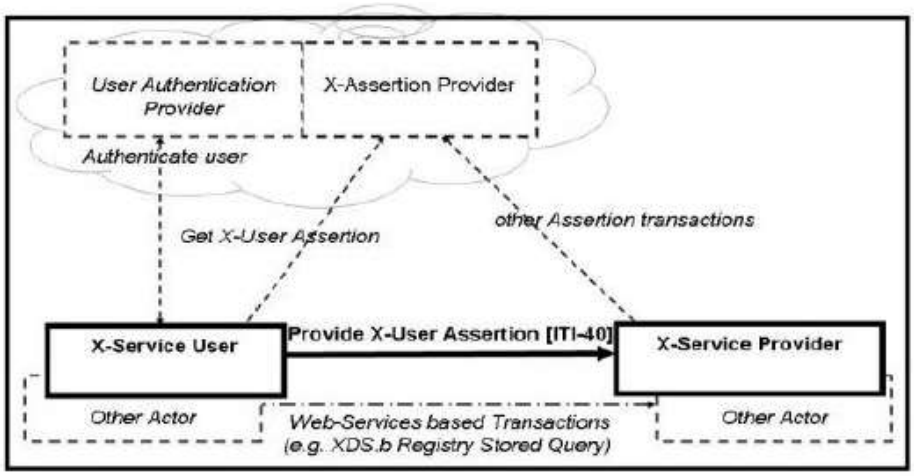

Abbildung 1: XUA Profil Akteure und Transaktionen

XUA spezifiziert die Verwendung eines Web-Services Security Headers mit einem Security Assertion Markup Language (SAML) 2.0 Token[10], lässt aber auch andere Möglichkeiten offen um die Identität des Users bereitzustellen, wenn die Interoperabilität durch Policies gesichert wird. Die Methode, um den User zu authentifizieren, und die Methode Get X-User Assertion werden von XUA nicht definiert. Im Kontext der Bürgerkartenameldung scheint allerdings MOA-ID zur Erfüllung dieser Aufgaben geeignet (siehe *Abschnitt 3*). Des Weiteren werden die Attribute, welche in der Identity Assertion benötigt werden, innerhalb des XUA Profils nicht definiert. Allerdings wurde 2010 ein Zusatz zum IT Infrastructure Technical Framework für Testimplementationen (Supplement for Trial Implementation) namens Cross-Enterprise User Assertion – Attribute Extension (XUA++) [6] veröffentlicht, welcher die Intentionen von IHE zum Thema Rollennachweis zeigt. XUA++ erweitert das XUA Profil um Optionen, die eine Zugriffskontrolle ermöglichen, wobei ein definierter Use-Case die rollenbasierte Zugriffkontrolle betrifft. Zu diesem Zweck wurden die beiden XUA Akteure um die Option Subject-Role erweitert. Wenn diese Option verwendet wird, hat der X-Service User seine relevante Rolle innerhalb eines SAML 2.0 Tokens in einem <saml:Attribute> Statement darzustellen.

Katt et. al. beschreiben in [7] eine von nationalen Gesetzgebungen unbeeinflusste Herangehensweise. International gesehen gilt es, die verschiedenen Bestrebungen zu beobachten. Dazu ist es erforderlich, die Anforderungen aus dem zukünftigem ELGA-Gesetz mit eID im Gesundheitswesen und der internationalen Harmonisierung von eIDs (wie im Large Scale Pilot STORK 0) in Verbindung zu bringen.

3. Methoden

Österreich hat die elektronische Identität (eID) in Form der Bürgerkarte, einer ID-Karte mit kryptographischen Funktionen, eingeführt. Im Zusammenhang mit eIDs ist die elektronische Signatur ein Schlüsselfaktor für die sichere und eindeutige Authentifizierung. Die rechtliche Grundlage für die Verwendung von elektronischen Signaturen ist das österreichische Signaturgesetz (SigG) (BGBl I Nr. 190/1999), welches die nationale Umsetzung der EU Directive für elektronische Signaturen 1999/93/EG [2] darstellt. Eine qualifizierte elektronische Signatur wird von einer sicheren Signaturerstellungseinheit (der Bürgerkarte) erzeugt und beruht auf einem qualifizierten Zertifikat. Das qualifizierte Zertifikat auf der Bürgerkarte wird von der Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr (A-Trust) nach einer Identitätsprüfung des Inhabers erzeugt und auf dem Chip der Bürgerkarte gespeichert. Die qualifizierte elektronische Signatur ist laut SigG der

handschriftlichen Unterschrift gleichzusetzen und eignet sich somit zur Authentifizierung von GDAs für den Zugriff auf sensible Gesundheitsdaten. Da im qualifizierten Zertifikat der Bürgerkarte lediglich der Name der Person festgehalten wird, verwendet die Bürgerkarte zur eindeutigen Identifizierung eine Personenbindung. Diese basiert auf der ZMR-Zahl (Identifikation im zentralen Melderegister ZMR) die zur Stammzahl umgerechnet wird. Eine Rückrechnung ist nicht möglich. Die Personenbindung ist eine XML-Struktur basierend auf der SAML 1.0 [9], welche neben der Stammzahl den Namen, das Geburtsdatum und den öffentlichen Schlüssel des qualifizierten Zertifikates enthält. Diese XML-Datei wird von der Stammzahlenregisterbehörde signiert und auf dem Chip der Bürgerkarte gespeichert. Die sichere Identifizierung und Authentifizierung von Benutzern mittels Bürgerkarte erfolgt über die in Open Source Lizenz bereitgestellte Softwarekomponente MOA-ID, welche sämtliche Identitäts-, Zertifikats- und Authentifizierungsprüfungen durchführt und relevante Anmeldedaten der nachfolgenden Online-Applikation zur Verfügung stellt. Online-Applikationen, welche MOA-ID verwenden, verweisen im Anmeldeprozess durch Links auf die Authentisierungskomponente von MOA-ID. Die Authentisierungskomponente beginnt mit dem Einholen personenbezogener Informationen. Nach dem Auslesen der Personenbindung und eventuell weiterer zusätzlicher Infoboxen validiert MOA-ID die Personenbindung und eventuelle Infoboxen. Nach erfolgreicher Prüfung wird eine XML-Struktur, der sogenannte AUTH-Block, aufgebaut, welcher vom Benutzer signiert wird. Die Authentisierungskomponente überprüft den signierten AUTH-Block und legt bei Erfolg für den Benutzer Anmeldedaten an. Anschließend wird der URL der Online-Applikation aufgerufen und ein eindeutiges Artefakt als Parameter übergeben. Unter Verwendung des übermittelten Artefakts kann die Online-Applikation die Anmeldedaten des Benutzers mittels eines SOAP-Requests abholen. Die XML-Struktur der Personenbindung, des AUTH-Blocks und der Anmeldedaten basiert auf der SAML. Um MOA-ID in Zukunft tatsächlich im Gesundheitswesen einsetzen zu können ist eine Hebung des Moduls auf SAML 2.0 Standard erforderlich.

Laut österreichischem E-Government-Gesetz (E-GovG) (BGBl I Nr. 10/2004) erfolgt in der Bürgerkarte eine eindeutige Identifikation von Personen durch ihre Stammzahl, die von einer Stammzahlenregisterbehörde (SZRB) verwaltet und geprüft wird. Das Auslesen der Personenbindung aus der Bürgerkarte ist durch einen PIN-Code geschützt. Innerhalb einer Datenanwendung darf die Identifikation von natürlichen Personen nur mittels des bereichsspezifischen Personenkennzeichens (bPK) vorgenommen werden. Die Stammzahl natürlicher Personen darf innerhalb einer Datenanwendung nicht gespeichert werden. Das bPK wird durch die Ableitung der Stammzahl gebildet. Dazu wird jenes Bereichskürzel der verschiedenen Verwaltungsbereiche (E-Government-Bereichsabgrenzungsverordnung (BGBl. II Nr. 289/2004)) verwendet, in welchem das bPK verwendet werden soll. Zur Identifikation von GDAs in Österreich wird in [3] der HPI vorgeschlagen, welcher durch die weitere Ableitung des bPK mit der Bereichskennung GH (bPK Gesundheit) gebildet wird. Damit ist im öffentlichen Bereich die Möglichkeit gegeben, den HPI zu berechnen. Bei der Verwendung der Bürgerkarte im privaten Bereich (z.B. Arztpraxen) wird allerdings das bPK mit der Stammzahl des privaten Anbieters anstelle der Bereichskennung berechnet. Aufgrund der Tatsache, dass somit die bPK Gesundheit im privaten Bereich nicht verfügbar ist, kann der HPI nicht direkt berechnet werden. Allerdings ermöglicht MOA-ID mittels gewisser Konfigurationsparameter für Anbieter aus dem privaten Bereich die Berechnung des HPI durch die BKU. Dadurch wird sowohl im öffentlichen als auch im privaten Bereich eine gleiche Identifikationsqualität erreicht, welche für die Nutzung zentraler Register (im Rahmen der Infrastruktur eines zukünftigen elektronischen Gesundheitsaktes – ELGA) notwendig ist.

4. Ergebnisse

Zentrales Ergebnis dieser Arbeit sind zwei Softwaremodule. Um Rollen von GDAs online abfragen zu können, wurde ein OnlineService für Rollen (OSR) entwickelt. Es erweitert das Rollen beinhaltende Register um die Abfrage von zugeordneten Rollen und eine Attestierungs-übermittlung. Das zweite Modul, MOA-GDA-R (MOA-GDA mit Registerabfrage), ist ein Erweiterungsmodul für MOA-ID. Es dient der Prüfung der Bescheinigung von Rollen und Kommunikation mit dem Rollenregister. Das OSR kommuniziert mit einer dahinter liegenden Datenbank, in welche von Bestandgebern über definierte Schnittstellen GDAs und deren Rollen eingetragen werden, bzw. in der durch GDAs selbst mittels eines Services beantragte und freigegebene Rollen enthalten sind. Das Register muss immer auf dem aktuellen Stand gehalten und durch entsprechende technische sowie organisatorische Sicherheitsmaßnahmen geschützt sein. Somit ist gesichert, dass alle im Register eingetragenen Rollen ihren aktuellen Status besitzen.

Damit wird die Problematik umgangen, Rollennachweise in der BKU speichern zu müssen, oder nicht mit BKUs arbeiten zu können, die keine Infoboxen außer der der Personenbindung unterstützen. Eine Übersicht der am Anmeldeprozess beteiligten Komponenten ist in *Abbildung 2* dargestellt. Das OSR ist als Erweiterung zu MOA-ID als eigenes optionales Modul verfügbar und in den Anmeldeprozess von MOA-ID integriert. Ein definierter Parameter weist MOA-ID darauf hin, das OSR zu kontaktieren. In diesem Konzept wird das Auslesen eines GDA-Tokens aus der Infobox einer BKU durch die online Abfrage der Rollen über das OSR ersetzt.

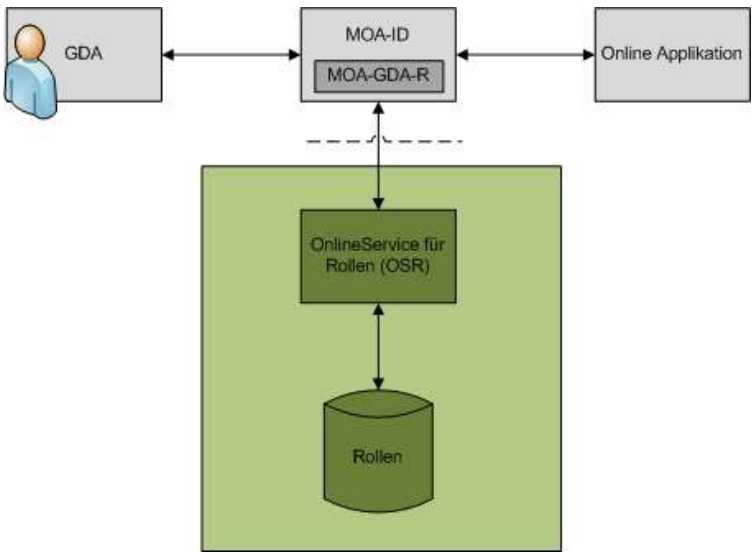

Abbildung 2: Komponenten OSR

Die Schnittstelle zwischen MOA-GDA-R und dem OSR wurde als SOAP WebService Schnittstelle implementiert und bietet die Funktionen EstablishSession, GetRole und GetSAMLAttribute. Der Ablauf des Anmeldeprozesses wird in *Abbildung 3* dargestellt.

Wie bei der standardmäßigen Anmeldung mittels MOA-ID wird zu Beginn des Anmeldeprozesses die Personenbindung des GDAs ausgelesen und verifiziert. Im nächsten Schritt kontaktiert MOA-GDA-R das OSR durch den Aufruf der EstablishSession Funktion, an welche die Personenbindung übergeben wird. Die Identifikation in der Personenbindung wird durch den HPI ersetzt. Im Behördenumfeld berechnet MOA-GDA-R den HPI je nach Konfiguration aus der Stammzahl oder dem bPk durch eine weitere Hashwert-Ableitung [1], im privaten Bereich übernimmt die BKU diese

Berechnung. Das OSR überprüft innerhalb der EstablishSession Funktion das von MOA-ID verwendete SSL-Zertifikat, ordnet nach erfolgreicher Validierung die Personenbindung einer eindeutigen SessionID zu und liefert die SessionID an MOA-ID zurück. Der Aufruf der Funktion GetRole mit der SessionID als Request Parameter bildet den nächsten Schritt im Anmeldeprozess. Das OSR kann aufgrund der SessionID die zu dem GDA passende Personenbindung finden und die in der Datenbank eingetragenen zugehörigen Rollen abfragen. MOA-GDA-R erhält als Antwort diese Liste von gültigen Rollen (Object Identifier (OID) und textuelle Beschreibung) für den entsprechenden GDA und zeigt diese Rollen dem GDA an. Der GDA kann aus dieser Liste eine oder mehrere Rollen wählen. Die gewählte(n) Rolle(n) werden gemeinsam mit der SessionID als Request Parameter an die Funktion GetSAMLAttribute übergeben. Das OSR überprüft die übermittelte Rolle und erzeugt nach erfolgreicher Validierung SAML-Attribut Statements.Um die Integrität des SAML-Attributes sicherzustellen, wird die XML-Struktur vom OSR signiert. Das signierte SAML-Attribut sowie die SessionID werden als Response Parameter an MOA-GDA-R übermittelt. MOA-ID kann aufgrund der Session-ID den GDA wieder dem laufenden Prozess zuordnen und diesen fortsetzen.

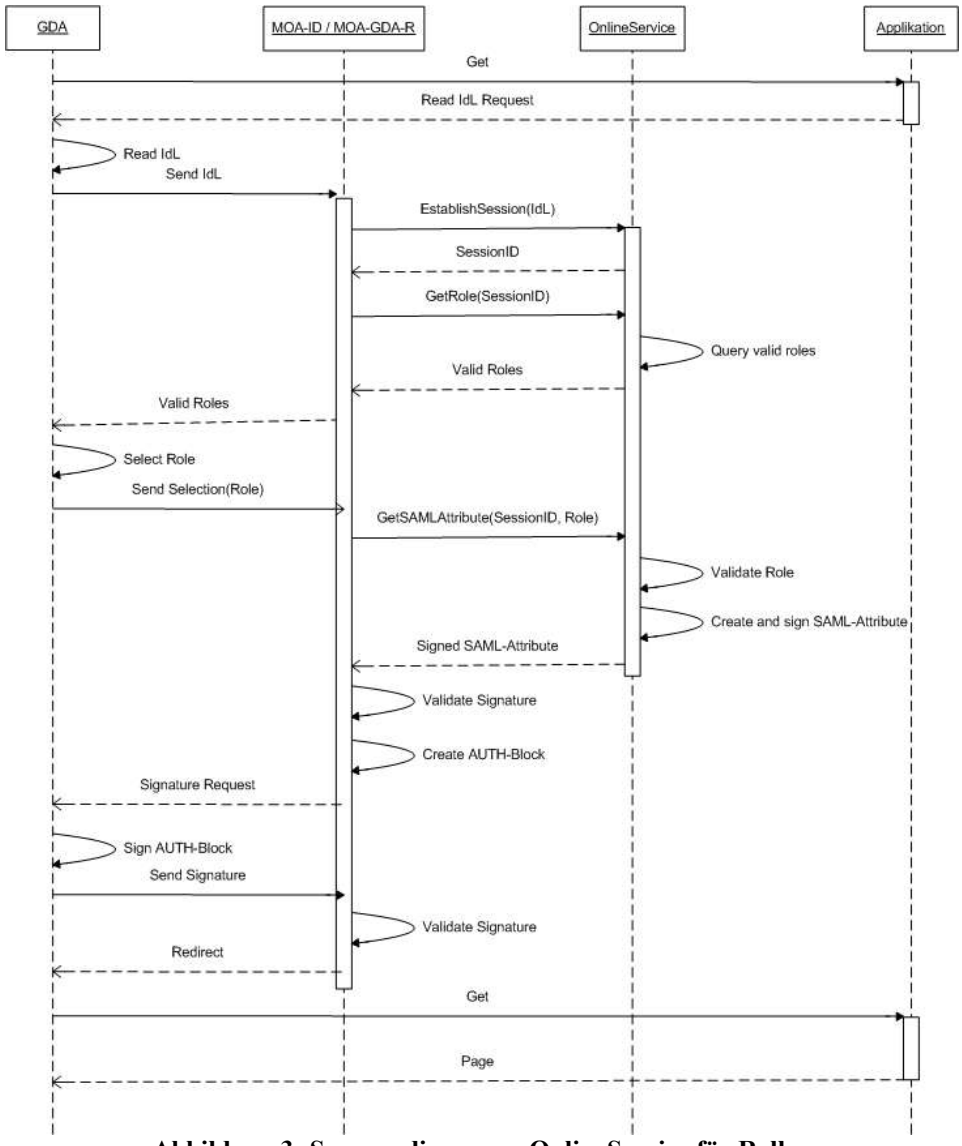

Abbildung 3: Sequenzdiagramm OnlineService für Rollen

MOA-ID erstellt zusammen mit der Personenbindung und dem zusätzlichen SAML-Attribut (Rolle) den AUTH-Block und erzeugt einen SignatureRequest welcher von dem GDA signiert wird. MOA-ID überprüft die Signatur. Nach erfolgreicher Authentifizierung wird der GDA an die nachfolgende Applikation weitergeleitet wobei sich die Applikation anschließend Anmeldedaten in Form einer SAML-Assertion mittels eines SOAP Requests bei MOA-ID abholen kann. Die Anmeldedaten enthalten die Informationen zur Rolle ebenfalls in einem <saml:Attribute> Statement, wobei aufgrund dieser Informationen von der nachfolgenden Applikation Zugriffsentscheidungen getroffen werden können.

5. Diskussion und Ausblick

Es gilt sicherzustellen, dass Denial of Service Attacken am OSR weitgehend vermieden werden. Ein wichtiger Schritt in diese Richtung kann der Einsatz von Client-Authentifizierung mit Zertifikaten sein. Dies würde jedoch bedeuten, dass ein hoher organisatorischer Aufwand betrieben werden muss, die jeweils neuen erlaubten Gesundheitsanwendungen an dem Rollenregisterzugriffs- punkt in den Truststore aufzunehmen. Eine andere Möglichkeit ist die Verwendung bestimmter Attribute in Clientzertifikaten, was den organisatorischen Aufwand hin zur Zertifikat ausstellenden Stelle verlagert. Wir gehen daher davon aus, dass das OSR zu Beginn eher ohne Client-Authentifizierung betrieben wird, da anders als im E-Government bei Behörden, die Zahl der anfragenden Stellen um ein vielfaches höher sein wird. Eine gesetzliche Regulierung der Zugriffe kann in Zukunft aber notwendig werden.

GDAs, welche mit ihren Rollen in der Datenbank des OSR eingetragen sind, sollten auf Anfrage eine elektronische Bescheinigung ihrer Identität und Rollen beantragen können. Hierfür bieten sich entweder elektronische Zertifikate oder die XML-Struktur GDA-Token an. Während der Aufbau und die Struktur von GDA-Token bereits definiert ist [1], stellt sich die Frage, wie Rollen in Zertifikaten abgebildet werden können. Eine zunächst angedachte Methode war die Abbildung von Rollen in X.509 Attributzertifikaten. Attributzertifikate können Public-Key-Zertifikaten (PK-Zertifikaten) zugeordnet und selbst ausgestellt werden, wodurch sie sich grundsätzlich für die Verwendung zur Abbildung von Rollen eignen. Allerdings werden Attributzertifikate in Österreich nicht verwendet, werden im SigG nicht geregelt und sind demnach laut SigG keine Zertifikate. Aufgrund dessen ist die Verwendung von Attributzertifikaten nicht für den Nachweis von Rollen geeignet. Für das OSR wurde die Abbildung von Rollen in X.509 PK-Zertifikaten gewählt, wobei in diesem Fall die Rollen in SubjectDirectoryAttributes oder in privaten Erweiterungen, wie sie im E-Government verwendet werden, abgebildet werden können. Für die Erstellung der X.509 Zertifikate muss eine Public-Key-Infrastructure (PKI) aufgebaut werden. Da die Schlüssel in den Rollenzertifikaten nicht verwendet werden, sei an dieser Stelle erwähnt, dass die ursprünglich geplante Form des Rollennachweises in Form des GDA-Tokens als optimalste Form angesehen werden kann.

Die Prozesse für eine qualifizierte Identifikation nach E-Government Konzepten sind bereits seit einigen Jahren verfügbar, jedoch wurde bisher keine weite Verbreitung erreicht. Durch das im Rahmen dieser Arbeit entstandene, von Bürgerkarteninfoboxen unabhängige System steht einer hohen Durchdringungsrate der qualifizierten Identifikation im extramuralen Bereich des Gesundheitswesens nichts mehr im Wege. Die Umsetzung, die das Ergebnis dieser Arbeit ist, sorgt des Weiteren dafür, dass auch heute zur Verfügung stehende BKUs eingesetzt werden können, deren Einsatz bisher mangels fehlender Infoboxmanipulationsmöglichkeiten nicht möglich war. Der Be-

darf ist mit geschätzten achtzigtausend betroffenen Ärzten und mehreren hunderttausend betroffenen anderen GDAs gegeben.

Wir hoffen, dass unsere Arbeit hilft, ein österreichweites, interoperables und sicheres Gesundheitsnetzwerk zu schaffen, welches es auch GDAs, die nicht an ein Gesundheitsnetzwerk angebunden sind, ermöglicht, Teil dieses Gesamtsystems zu sein.

6. Literatur

[1] DANNER P., RÖSSLER T., KNALL T., GDA-Token Spezifikation, Version 1.0.1., Graz 2008.

[2] EUROPÄISCHES PARLAMENT, RAT DER EUROPÄISCHEN UNION, Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, 1999/93/EG, Dezember 1999, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:de:HTML.

[3] Gesundheitstelematikverordnung, Begutachtungsentwurf, https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Begut&Dokumentnummer=BEGUT_COO_2026_100_2_464278.

[4] HOLLOSI A., KARLINGER G., RÖSSLER T., CENTNER M., Die österreichische Bürgerkarte Version 1.2, Konvention, 2008, http://www.buergerkarte.at/konzept/securitylayer/spezifikation/20080220/.

[5] IHE, IT Infrastructure Technical Framework, Revision 7.0, August 2010, http://www.ihe.net/Technical_Framework/index.cfm#IT.

[6] IHE, IT Infrastructure Technical Framework Supplement, Cross-Enterprise User Assertion – Attribute Extension (XUA++), August 2010, http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XUA-_Rev1-1_TI_2010-08-10.pdf.

[7] KATT B. et.al., Privacy and Access Control for IHE-based Systems, eHealth 2008, London 2008.

[8] LEITOLD H., HOLLOSI A., POSCH R., Security Architecture of the Austrian Citizen Card Concept, in: ASAC ´02: Proceedings of the 18th Annual Computer Security Applications Conference, Washington, CD, USA: IEEE Computer Society, 2002, p.391.

[9] OASIS, Assertions and Protocol for the OASIS Security Assertion Markup Language v1.0, http://www.oasis-open.org/committees/security/docs/cs-sstc-core-01.pdf.

[10] OASIS, Assertions and Protocol for the OASIS Security Assertion Markup Language v2.0, http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.

[11] SCHAMBERGER R., KARLINGER G., MOSER L., Spezifikation MOA ID 1.4, Wien/Graz, 2007, http://egovlabs.gv.at/.

[12] STORK, Secure idenTity acrOss boRders linKed, EU, 2011, https://www.eid-stork.eu.

[13] IVKOVIC M., KESKEL U., ET.AL., STORK WORK Item 3.3.6 - Mobile eID, 2010, https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1385.

Corresponding Author

Peter Danner
exthex GmbH
Göstinger Straße 213, A-8051 Graz
Email: peter.danner@exthex.com